WHAT IS CLAIMED IS:

1. A method of providing secure communication in a network, said method comprising:

providing an instruction set in response to a request by a sending computer for secure communication wherein said instruction set is executed by a receiving computer when a predetermined condition is met; and

disabling said instruction set upon verification of identifying user information received from said receiving computer.

2. The method of claim 1 wherein said providing step includes the step of selecting one or more instruction sets from a group of instruction sets comprising instructions for destroying a communication and its accompanying instruction set, instructions for removing selected information from said receiving computer, and instructions for transmitting information from said receiving computer.

3. The method of claim 1 wherein said predetermined condition is the failure of the receiving computer to decrypt an encrypted communication received from said sending computer.

4. The method of claim 1 wherein said disabling step includes the step of comparing said identifying user information against a list of identifying user information wherein said identifying user information uniquely identifies a user.

5. The method of claim 1 wherein said identifying user information is a biometric identifier.

6. The method of claim 1 further comprising:

receiving an encrypted communication and instruction set from a receiving computer;

verifying identifying information provided by said receiving computer;

decrypting said encrypted communication upon successful verification of said identifying information; and

transmitting said decrypted communication to said receiving computer.

7. A computer system for providing secure communication in a networked environment, the computer system comprising:

a central processing unit;

a memory, coupled to said central processing unit, said memory storing:

a list of instruction sets wherein instructions in said instruction set are performed by a receiving computer;

a database containing identifying user information wherein said identifying user information uniquely identifies a user; and

a secure communication module comprising:

instructions for providing an instruction set in response to a request for secure communication by a sending computer wherein said instruction set is executed by said receiving computer when a predetermined condition is met; and

instructions for disabling said instruction set upon verification of said identifying user information received from said receiving computer.

8. The computer system of claim 7 wherein said providing instructions include instructions for selecting one or more instruction sets from a group of instruction sets comprising instructions for destroying a communication and its accompanying instruction set, instructions for removing selected information from said receiving computer, and instructions for transmitting information from said receiving computer.

9. The computer system of claim 7 wherein said predetermined condition is the failure of said receiving computer to decrypt an encrypted communication received from said sending computer.

10. The computer system of claim 7 wherein said instructions for disabling said instruction set include instructions for comparing said identifying user information against said database of identifying user information.

11. The computer system of claim 7 wherein said identifying user information is a biometric identifier.

12. The computer system of claim 7 wherein said secure communication module further includes:

instructions for receiving an encrypted communication and instruction set from a receiving computer;

instructions for verifying identifying user information provided by said receiving computer;

instructions for decrypting said encrypted communication upon successful verification of said identifying user information; and

instructions for transmitting said decrypted communication to said receiving computer.

13. A computer software program for use in conjunction with a computer system, the computer program comprising a computer-readable storage medium and a computer program mechanism embedded therein, the computer program mechanism comprising:

a list of instruction sets wherein instructions in said instruction set are performed by a receiving computer;

a database containing identifying user information wherein said identifying user information uniquely identifies a user; and

a secure communication module comprising:

instructions for providing an instruction set in response to a request for secure communication by a sending computer wherein said instruction set is executed by a receiving computer when a predetermined condition is met; and

instructions for disabling said instruction set upon verification of said identifying user information received from said receiving computer.

14. The computer software program of claim 13 wherein said providing instructions include instructions for selecting one or more instruction sets from a group of instruction sets comprising instructions for destroying a communication and its accompanying instruction set, instructions for removing selected information from

said receiving computer, and instructions for transmitting information from said receiving computer.

15. The computer software program of claim 13 wherein said predetermined condition is the failure of said receiving computer to decrypt an encrypted communication received from said sending computer.

16. The computer software program of claim 13 wherein said instructions for disabling said instruction set include instructions for comparing said identifying user information against said database of identifying user information.

17. The computer software program of claim 13 wherein said identifying user information is a biometric identifier.

18. The computer software program of claim 13 wherein said secure communication module further includes:

instructions for receiving an encrypted communication and instruction set from a receiving computer;

instructions for verifying identifying information provided by said receiving computer;

instructions for decrypting said encrypted communication upon successful verification of said identifying information; and

instructions for transmitting said decrypted communication to said receiving computer.